

Risicoverslaggeving in het directieverslag in beweging

Marijn van Daelen en Jos de Groot

SAMENVATTING Sinds 2004 vraagt de Nederlandse Corporate Governance Code (hierna Code) beursgenoteerde organisaties om in de risicoparagraaf in het jaarverslag specifieke informatie te verschaffen over de voornaamste risico's, het risicobeheersings- en controlesysteem en een In-control verklaring af te geven. De afgelopen tien jaar zijn met regelmaat publicaties verschenen die aangeven dat de risicoparagraaf nog te weinig informatief is. In dit artikel wordt de balans opgemaakt van hoe de 50 AEX- en Midcap-fondsen in de jaarverslagen 2013 inhoud hebben gegeven aan de risicoparagraaf in relatie tot actuele verwachtingen van stakeholders over de inhoud van de risicoparagraaf. De uitkomsten van het onderzoek en daarop gebaseerde aanbevelingen zijn bedoeld om de opstellers van het jaarverslag en de interne toezichthouders (de commissarissen) nadere handvaten te geven voor het opstellen van een risicoparagraaf over het boekjaar 2014.

RELEVANTIE VOOR DE PRAKTIJK Risicoverslaggeving in het jaarverslag staat in de schijnwerpers. Dit artikel laat de resultaten zien van ons onderzoek naar de risicoparagraaf in de jaarverslagen van AEX en Midcap fondsen. Het onderzoek richt zich op de informatie die deze ondernemingen in de risicoparagraaf 2013 rapporteren en of deze ondernemingen met hun risicoparagraaf tegemoet komen aan de wensen van stakeholders. Op basis hiervan geven wij aanbevelingen voor opstellers van de risicoparagraaf en voor interne toezichthouders.

1 Risicoverslaggeving in schijnwerpers

De risicoparagraaf in het jaarverslag vindt zijn wettelijke basis in artikel 2:391 BW waarin is bepaald dat het wettelijke verplichte jaarverslag een beschrijving bevat van de voornaamste risico's en onzekerheden waarmee de rechtspersoon wordt geconfronteerd. De risicoparagraaf bestaat uit drie met elkaar samenhangende elementen (De Groot, 2010). Ten eerste het risicoprofiel. Het risicoprofiel van de organisatie is een uiteenzetting van de belangrijkste operationele, strategische, financiële, wet- en regelgevingsrisico's en rapportagerisico's waaraan een organisatie blootstaat. Ten tweede

de beschrijving van het risicomanagementsysteem waarin de karakteristieken worden uiteengezet van het organisatie-specifieke systeem van risicomanagement waarmee de bedrijfsrisico's worden beheerst. Ten slotte de In-control-verklaring, een uitspraak van de organisatieleiding over de opzet en/of de werking van het systeem van risicomanagement.

Deze driedeling komt terug in de in 2003 door de toenmalige Commissie Tabaksblat opgestelde Nederlandse Code Corporate Governance. De Code is op 1 januari 2004 in werking getreden en in december 2008 geactualiseerd door de Commissie Frijns. In het bijzonder komt de risicoparagraaf terug in best practice-bepaling II.1.4 inzake het risicoprofiel en de beschrijving van het organisatiebrede risicomanagementsysteem. In best practice-bepaling II.1.5 inzake de In-control-verklaring komt de effectieve opzet en werking van de interne beheersing rondom financiële verslaggevingrisico's terug. Het toezicht van de commissarissen op het risicoprofiel en het risicomanagement krijgt specifieke aandacht in best practice-bepaling III.1.8 in de Code.

De Nederlandse Code is destijds in belangrijke mate geïnspireerd op de UK Combined Code. In de UK is recent actief gekeken naar hoe die Code toekomstig bestendiger gemaakt kan worden. De Financial Reporting Council (FRC) heeft na een consultatieronde, in september 2014 een geactualiseerde UK Combined Code gepubliceerd. Tegelijkertijd met de aanpassing van die Code is een nadere guidance uitgebracht: 'Guidance on Risk Management, Internal Control and related Financial and Business Reporting'. In de nieuwe voorschriften wordt onder andere de rol van het bestuur ten aanzien van het definiëren van de risicohouding ('risk appetite' of risicoappetijt) zwaarder aangezet. Er wordt gevraagd om een robuuste beoordeling van het risicoprofiel, inclusief die factoren die de solvabiliteit, de liquiditeit, het 'business model' of toekomstige prestaties bedreigen. Ook moet het bestuur in haar verslag uiteenzetten dat die analyse is uitgevoerd en aangeven op welke wijze de voornaamste risico's worden beheerst of gemitigeerd. Ook dient het bestuur ten minste één keer per jaar een beoordeling uit te voeren van de effectiviteit van het systeem van

risicobeheersing en internal control en in het jaarverslag beschrijven dat die beoordeling is uitgevoerd. Tevens dient uiteengezet te worden of er materiële onzekerheden zijn in relatie tot de verslaglegging op basis van de continuïteitsverwachting voor ten minste de komende twaalf maanden.

De recente Nederlandse aanpassing van de Richtlijn voor de Jaarverslaggeving 400 (hierna RJ400) is ook een stap in de goede richting maar gaat minder ver dan de UK-plannen. De RJ400-aanpassingen (met als ingangsdatum de jaarverslagen over 2015) vragen om een uiteenzetting van de risicohouding, de wijze waarop individuele risico's tegemoet worden getreden (de zogenaamde risico-respons), de beschrijving van de impact van de risico's op de resultaten en/of financiële positie, welke risico's het afgelopen jaar een belangrijke impact hebben gehad en de gevolgen daarvan, alsmede welke verbeteringen in het systeem van risicomanagement zijn aangebracht.

Dit soort aanpassingen in wet- en regelgeving en codes staan niet op zichzelf. Het is het antwoord op de kritiek en vragen van stakeholders naar informatievere informatievoorziening over risico's en risicomanagement. In de speerpuntenbrieven van de Vereniging van Effectenbezitters (VEB, 2013) en Eumedion (Eumedion 2013, 2014) van de afgelopen jaren komt dit structureel terug.

De extra aandacht past ook in de trend waarin integrated reporting meer aandacht krijgt. Centraal in die nieuwe vorm van verslaggeving staan de maatschappelijke bestaansrede van de organisatie, de missie, de strategie, de waardecreënde activiteiten en de voornaamste risico's die dit in de weg kunnen staan. De expliciete link tussen langetermijnstrategie en risico's, alsmede het benoemen van de effecten van risico's blijft vaak nog achterwege, zo toont onderzoek naar de jaarverslagen 2012 aan (Deloitte, 2013).

Ook de nieuwe controleverklaring van de externe accountant, waarmee in 2013 is geëxperimenteerd en die volgens de voorstellen van de Nederlandse Beoepsorganisatie van Accountants (NBA, 2014) met ingang van 2014 verplicht zal gaan worden voor alle Organisaties van Openbaar Belang (OOB), leidt ertoe dat de risicoparagraaf alsmede het verslag van de Raad van Commissarissen extra aandacht gaan krijgen. Uit onderzoek (PwC, 2014) blijkt namelijk dat in een derde van de gevallen in de controleverklaring van de externe accountant risicofactoren rondom de financiële verslaglegging worden genoemd die niet als zodanig expliciet terugkomen in de risicoparagraaf in het jaarverslag. Dit is een onwenselijke situatie aangezien de informatievoorziening door de externe accountant nooit de vervanger kan zijn van informatie die in eerste instantie door het bestuur en commissarissen verstrekt moet worden (Brouwer & De Groot, 2014).

In dit artikel is gekozen voor een thematisch onderzoek op basis van actuele thema's in regelgeving en uitingen van stakeholders. In paragraaf twee wordt de reikwijdte en de aanpak van het onderzoek naar de risicoparagraaf nader uitgewerkt. Paragraaf drie bevat vervolgens de uitkomsten van het onderzoek, waarbij tevens voorbeelden worden genoemd van good practices in de jaarverslagen 2013. Paragraaf vier geeft enkele aanbevelingen aan de opstellers van en interne toezichthouders op de risicoparagraaf in het jaarverslag.

2 Afbakening en aanpak van het onderzoek

Dit onderzoek richt zich op de risicoparagraaf in het jaarverslag over 2013. Buiten de scope van het onderzoek valt de informatie over risico's en risicomanagement in het verslag van de Raad van Commissarissen (RvC) en de toelichtingen over risico's in de jaarrekening (waaronder bijvoorbeeld de IFRS7-toelichtingen ten aanzien van de risico's van financiële instrumenten). De onderzoekspopulatie bestaat uit de 50 AEX- en AMX-ondernemingen met peildatum 1 januari 2014 (zie bijlage A).

Diverse onderzoeken, raamwerken en recent beschreven ontwikkelingen bieden inzicht in de wensen van stakeholders. Zo blijkt uit onderzoek van Van Daelen (2012) dat er ruimschoots aanwijzingen zijn ten aanzien van de risico-informatie die in de optiek van beroepsorganisaties, belangenorganisaties, beleidsmakers en aandeelhouders gepubliceerd zou moeten worden. Waar het idee kan ontstaan dat er een grote verscheidenheid is in de vraag naar elementen van risico-informatie in verschillende rapporten en door de jaren heen, geeft dit onderzoek het geruststellende beeld dat veel elementen – weliswaar in steeds variërende samenstellingen – herhaaldelijk en tevens in diverse landen benoemd worden. Met een analyse van de elementen die keer op keer worden aangeduid als belangrijk, worden de bouwstenen voor risicorapportage zichtbaar. Tezamen vormen deze tien bouwstenen het gewenste format voor de openbaarmaking van risico-informatie. De tien elementen van risico-informatie die een dergelijk format voor risicorapportage zou moeten bevatten zijn de volgende: (1) categoriseren van risico's, (2) benoemen van de voornaamste risico's, (3) de ondernemings-specifieke risico's, (4) geven van een gedetailleerde beschrijving, (5) toespitsen op materiële informatie, (6) duiden van de waarschijnlijkheid dat risico's materialiseren en (7) de potentiële impact, (8) prioriteren van de risico's, (9) aangeven van de risicomitigatie en (10) de risicobereidheid van de onderneming. Bij risicorapportage conform deze bouwstenen is het van belang dat de openbaargemaakte risico-informatie vooral op haar waarde kan worden geschat indien de samenhang tussen risico's en de benadering van het geheel van risico's, tevens in relatie tot de strategie, wordt besproken. Dit ondersteunt de juiste in-

terpretatie van de openbaargemaakte risico-informatie en geeft een meer volledig beeld van de risicosituatie van de onderneming (Van Daelen, 2013). Uit onderzoek van De Groot (2010) blijkt dat naast bovengenoemde elementen tevens (a) het verbinden van individuele risico's aan de strategische doelstellingen, (b) het gebruik van heldere en leesbare taal en (c) het transparant zijn over fouten en verstoringen in de beheersing van specifieke risico's, bijdragen aan een risicoprofiel in het jaarverslag dat informatief is voor stakeholders. Op basis van onze eigen praktijkervaringen zien wij tevens in de interne risicorapportages het belang van het aangeven van de trend van de risico's in de tijd als een relevant rapportage-element, welk element ook voor de externe risicorapportage relevant kan zijn.

Naast het risicoprofiel bestaat, zoals eerder geschetst, de risicoparagraaf ook uit de beschrijving van het risicomanagementsysteem en de In-control-verklaring. In die beschrijving van het risicomanagementsysteem gaat het niet zozeer om de statische informatie over hoe een organisatie inhoud geeft aan haar risicomanagement, maar vooral om de risicohouding, de voornaamste aangebrachte en/of geplande verbeteringen in het systeem, alsmede over de geconstateerde tekortkomingen in die systemen. Juist dit soort aspecten krijgt dan ook aandacht in de Code en vernieuwde RJ 400 waarin stakeholderverwachtingen zijn verwoord. De In-control-verklaring is voor Nederlandse ondernemingen voorgeschreven in best practice-bepaling II.1.5 in de Code. Deze kent een heel specifieke scope, namelijk de beheersing van de financiële verslaggevingsrisico's. Relevant voor stakeholders is derhalve of die scope in de praktijk wordt gevolgd en hoe eventuele tekortkomingen in het systeem van risicomanagement zich vertalen in de bewoordingen van de In-control-verklaring.

Het onderzoek richt zich daarom op de informatie die ondernemingen in de risicoparagraaf 2013 rapporteren en of de onderzochte ondernemingen met hun risicoparagraaf tegemoet komen aan de hiervoor uiteengezette wensen van stakeholders. Hierbij is gekozen voor een thematisch onderzoek op basis van actuele thema's in regelgeving en uitingen van stakeholders. Deze thema's zijn kort samengevat:

- Voor het risicoprofiel (paragraaf 3.1): (1) risico en strategie, (2) toprisico's, (3) kwantificering, (4) risicohouding, (5) risicorepons, (6) risicotrend, (7) black box-risico's.
- Voor wat betreft de beschrijving van het risicomanagementsysteem (paragraaf 3.2) wordt ingezoemd op de thema's: (1) de verbeteringen c.q. veranderingen in de risicomanagementsystemen en (2) de gerapporteerde tekortkomingen in risicomanagementsystemen.
- Ten slotte zijn de onderzochte thema's van de In-

control-verklaring (paragraaf 3.3): (1) de reikwijdte qua risicogebieden, (2) de conclusie over de effectieve werking en (3) het effect van tekortkomingen op de bewoordingen van de In-control-verklaring.

3 Uitkomsten van het onderzoek

3.1 Het risicoprofiel

3.1.1 Strategische dimensie onderbelicht: strategie en risico vaak niet expliciet gekoppeld

In haar definitie voor integraal risicomanagement benadrukt De Nederlandsche Bank (2011) dat dit een interactief proces betreft van (1) het opstellen van de strategie en hieraan gekoppeld het risicoprofiel en de risicobereidheid, (2) het identificeren van risico's, (3) het opstellen en implementeren van het beleid voor risicobeheersing, tot (4) de uitvoering, monitoring en terugkoppeling over risico's en beheersmaatregelen. Uit de onderzochte risicoparagrafen blijkt dat de rapportage over het interne risicobeheersings- en controlesysteem doorgaans nog niet op basis van deze invalshoek plaatsvindt.

Het onderzoek bevat de vraag of in het jaarverslag een expliciete link wordt gelegd tussen de individuele risico's en de individuele strategische doelen. De uitkomsten tonen aan dat 20% van de jaarverslagen in meerdere of mindere mate die expliciete link laat zien. Een voorbeeld daarvan wordt gegeven in het jaarverslag van Koninklijke Ahold N.V. (zie figuur 1), waarin de strategie als uitgangspunt wordt genomen voor het geven van inzicht in de voornaamste risico's van de onderneming, inclusief drivers, mitigerende acties en potentiële impact daarvan op de onderneming. Op basis van onze praktijkervaringen verwachten wij dat integrated reporting een aanjager zal zijn voor het explicieter gaan koppelen van strategische doelstellingen, waardecreatie en individuele risico's.

In figuur 1 is tevens te zien hoe Koninklijke Ahold N.V., naast de link tussen strategie en risico, per risico aangeeft in welke risicocategorie het desbetreffende risico valt. De gebruikte risicocategorieën weerspiegelen het COSO Enterprise Risk Management (ERM) raamwerk: strategic (S), operational (O), financial and reporting (F) en compliance (C). Dit vormt een interessante en compacte informatievervalsing die tegemoet komt aan de traditionele risicocategorisering en toekomstgerichte strategie-gerelateerde rapportage. Een ander goed voorbeeld is te vinden in de risicoparagraaf van Corio 2013 (p. 69). Uit het onderzoek blijkt dat 88% van de onderzochte risicoparagrafen een uitsplitsing van risico's laat zien, doorgaans op basis van de bovengenoemde COSO-uitsplitsing. Deze categorisering geeft duidelijkheid en structuur aan het risicoprofiel.

Figuur 1 Voorbeeld: de link tussen strategie en risico's in jaarverslag 2013 van Koninklijke Ahold N.V., p. 65**How we manage risk (continued)****Ahold's principal risks and uncertainties¹**

Strategy	Description of risk	Key risk drivers	Risk mitigating actions	Potential consequence
Better place to shop	Information security (D) A lack of security around, or non-compliance with, privacy requirements for customer data might negatively impact strategic initiatives relating to customer loyalty	- Consumer confidence - Sensitivity of data - Privacy regulations - Use of third parties to process and store data - Global security threats - Growth of online sales	- Strategic and tactical information security policy and guidelines - Information security governance - Control standards for information management and security - Payment Card Industry (PCI) and privacy compliant control framework - Information security capabilities - Information security awareness program - Cyber insurance coverage	Ahold's business operations generate and maintain confidential commercial and personal information concerning customers, employees, suppliers and the Company. Disclosure of confidential information to unintended third parties may negatively impact Ahold's corporate reputation and competitive position or result in litigation or regulatory action. This could have a material adverse effect on Ahold's financial position.
Simplicity	Legislative and regulatory environment (C) A changing legislative and regulatory environment increases the cost of doing business, tax levels and the complexity of our operations	- Compliance deadlines - Increased and targeted enforcement - Government budget deficits - Public opinion / pressure	- Knowledge and awareness of regulations - Monitoring, review and reporting on changes - Operational procedures and guidance	Ahold's activities are subject to various laws and regulations in each local market where it operates. The cost of compliance with any of these laws could impact Ahold's operations and reduce its profitability. See further discussion of consequences of the legislative and regulatory risks below.
Responsible retailing	Product safety (D, C) Customers might become injured or ill from the consumption of own-brand products or other food or non-food products, or as a result of food fraud in the supply chain	- Internationalization of the supply chain - Customer trust in brands - Incidents across the world - Increased number of own-brand products - Speed of communications	- Product safety policies - Control standards for food and non-food products - Standard operating procedures - Dedicated product integrity departments at Corporate Center and both continents - Monitoring of continental performance - Third-party certification	Though it has mitigating actions in place, Ahold may face product safety problems, including disruptions to the supply chain caused by food-borne illnesses and negative consumer reaction to incidents, which may have a material adverse effect on the Company's reputation, results of operations and financial position.

3.1.2 Het blijft zoeken naar de echte top risico's

Uiteraard maakt elke onderneming een weloverwogen afweging van de risico's en worden de voornaamste risico's gerapporteerd. De meerderheid van de onderzochte risicoparagrafen (62%) geeft als voornaamste risico's in de risicoparagraaf 12 of meer risico's weer. Dit kan gezien worden als een vrij ruime interpretatie van het begrip 'voornaamste', ook al is er geen definitie c.q. norm voor wat het aantal te benoemen voornaamste risico's (toprisico's) is; derhalve is de door ons gehanteerde grens van 12 risico's een subjectieve grens. We hadden ook, zoals in het verleden al eens is geopperd door vertegenwoordigers van beleggers, een top 3 of top 5 aan risico's kunnen benoemen. Een aantal ondernemingen (38%) gaat een stapje verder. Zij geven

bijvoorbeeld concreet aan (a) dat zij uitsluitend de toprisico's rapporteren en benoemen er niet meer dan tien (6%) of (b) vermelden dat niet expliciet maar geven niet meer dan tien risico's weer (8%). Ook zijn er ondernemingen die (c) aangeven welke van de gerapporteerde voornaamste risico's zij zien als de echte toprisico's (24%).

Een voorbeeld van deze laatste variant wordt gegeven in de risicoparagraaf van het jaarverslag van PostNL N.V. (zie figuur 2). In haar risicoparagraaf beschrijft PostNL N.V. zeventien risico's verdeeld over de categorieën strategisch, operationeel, juridisch en financieel risico's. Van deze zeventien risico's zijn vijf risico's grijs gemarkeerd om aan te geven dat PostNL specifiek aan deze risico's aandacht zal geven. Een an-

Figuur 2 Voorbeeld top risico's uit jaarverslag 2013 van PostNL N.V., p. 44

Risk	Risk response
Strategic risks	
USO regulation As provider of Universal Postal Services, changes in USO regulation could have an adverse impact on PostNL's ability to adapt to market developments and changes in customer demand in a timely and effective way.	PostNL is in a continuous dialogue with government, decision makers and regulators to enhance its position as designated provider.
Substitution The increasing substitution of alternatives for PostNL's delivery services could reduce revenues and profitability.	PostNL continuously and consistently takes commercial initiatives to slow down or adapt to substitution. Furthermore, PostNL develops operational processes to adapt more flexibly to future volume declines.
Competition Competition may put pressure on market share, volumes and prices, which could have an adverse effect on PostNL's revenues and/or profitability.	Commercial initiatives are in place such as differentiation in service levels, (new) products and adequate pricing.
PostNL may decide to exit certain businesses or markets in the future, which could result in additional costs related to the discontinuation of operations, impairment of goodwill or other contractual liabilities.	The decision to exit, if contemplated, is reviewed by the Board of Management and the Supervisory Board. If it is approved, an exit plan is then made to limit the (financial) impact for relevant stakeholders involved.

der voorbeeld wordt gegeven door Koninklijke DSM N.V., die in haar risicoparagraaf eerst in een tabel haar top-vijf-risico's beschrijft met bijbehorende mitigerende acties en daaronder een beschrijving geeft van de negen andere voorname risico's die zij loopt (DSM, jaarverslag 2013, p. 118 e.v.).

3.1.3 Kwantificering: relevant maar gemakkelijker gezegd dan gedaan

Risicomanagement behelst niet alleen het identificeren en prioriteren van risico's maar ook het kwantificeren van risico's. Sommige risico's laten zich niet goed kwantificeren (denk bijvoorbeeld aan indirecte schade aan de reputatie van de onderneming), of slechts binnen een bepaalde bandbreedte kwantificeren (Deloitte, 2009). Uit het onderzoek blijkt dan ook dat de kwantificering van risico's zelden in de risicoparagraaf wordt besproken. Waar dat wel gebeurt, betreft het een selectief groepje risico's, veelal de financiële risico's. Ondanks de moeilijkheid van kwantificering heeft het wel de potentie in zich om de informatieve waarde van de beschrijving van risico's positief te beïnvloeden, aldus de toelichting op best practice-bepaling II.1.4 in de Nederlandse Corporate Governance Code. Een voorbeeld van kwantificering wordt onder andere gegeven in het jaarverslag van ING Groep N.V. De risicoparagraaf in dit jaarverslag laat een tabel zien waarin de middelen zichtbaar worden gemaakt die nodig zijn om specifieke risico's af te dekken (zie figuur 3).

3.1.4. Risicohouding blijft vaak onbenoemd of onderbelicht

De houding van de onderneming ten opzichte van de gesignaleerde risico's biedt een relevant inzicht aan de stakeholders. Het kan zijn dat de ene onderneming, bij een gelijkwaardig risico, meer bereid is om dat risico te lopen dan een andere onderneming. Deze mate van

honger naar het nemen van risico's, de risicoappetijt, bepaalt de strategie van de onderneming in het accepteren van risico's, de keuze voor de risicorespons en daarmee het nettorisico (restrisico na de risicorespons). Het is juist dit nettorisico dat echt interessant is voor stakeholders. Ondernemen is risico's nemen, dat is bekend. De risicorespons komt hierna aan bod. De eerste vraag is hoeveel risico de onderneming acceptabel vindt; hoeveel de onderneming in potentie wil riskeren. Het belang van deze informatie wordt onderstreept in de Code. De Code geeft in de toelichting op best practice-bepaling II.1.4 aan dat de onderneming in haar beschrijving van de voornaamste risico's voor de uitvoering van haar strategie, tevens aandacht moet besteden aan haar houding ten opzichte van de risico's, oftewel de risicoappetijt.

De uitkomsten van het onderzoek laten zien dat slechts 40% van de onderzochte ondernemingen in meerdere of mindere mate informatie over haar risicoappetijt publiceert in de risicoparagraaf. Hierbij dient te worden opgemerkt dat het percentage onder AEX-genoteerde ondernemingen aanzienlijk hoger ligt (52%) dan onder AMX-genoteerde ondernemingen (28%). Eerder onderzoek naar jaarverslagen over boekjaar 2006 en 2010 liet lagere percentages zien (Van Daelen, 2012). Dit lijkt erop te duiden dat het verschaffen van informatie over de risicohouding van de onderneming een opkomende ontwikkeling is, die vooral wordt ingezet door de AEX-genoteerde ondernemingen.

Ondanks dit verschil tussen de AEX- en AMX-ondernemingen, ligt hier voor beide groepen ondernemingen een duidelijke verbeterpotentie naar de toekomst toe. Een voorbeeld van een korte, heldere duiding van de houding van de onderneming ten opzichte van de categorieën van risico's, wordt gegeven in het jaarver-

Figuur 3 Voorbeeld kwantificering uit jaarverslag 2013 van ING Groep N.V., p. 257

Economic and Regulatory Capital (Bank diversified only) by risk type				
	Economic Capital		Regulatory Capital	
	2013	2012	2013	2012
Credit risk	18,009	11,875	19,074	18,684
Add-on credit risk	6,431	4,248		
Market risk	4,729	6,326	704	772
Business risk	1,773	1,837		
Operational risk	1,571	1,763	2,822	2,836
Total banking operations	32,513	26,049	22,600	22,292

Economic and Regulatory Capital (Bank diversified only) by business line combination				
	Economic Capital		Regulatory Capital	
	2013	2012	2013	2012
Commercial Banking	8,156	8,019	10,174	9,897
Retail Banking Benelux	5,242	4,155	7,015	5,679
Retail Banking International	6,091	6,518	5,155	6,028
Corporate Line Bank ⁽¹⁾	6,593	3,109	256	688
Unallocated	6,431	4,248		
Total banking operations	32,513	26,049	22,600	22,292

⁽¹⁾ Corporate Line includes funding activities at ING Bank level, internal transactions between business units and the Corporate Line, and is managed by Capital Management.

slag van TNT Express N.V. (zie figuur 4). Dit jaarverslag laat zien dat de Raad van Bestuur de risicoappetijt heeft geformaliseerd. Zij heeft hierbij gebruik gemaakt van de risicocategorieën van het COSO ERM-raamwerk en per categorie de risicoappetijt aangeduid, variërend van moderate, via low tot zero tolerance. De risicoparagraaf vervolgt met een overzicht van de voornaamste specifieke en inherente risico's per COSO ERM-risicocategorie en vervolgens mitigerende acties, waardoor zichtbaar is hoe het risicoprofiel van de onderneming doorwerkt in de feitelijke omgang met de risico's.

Figuur 4 Voorbeeld risicohouding uit jaarverslag 2013 van TNT Express N.V., p. 67

Risk appetite table		
Risk category	Category description	Risk appetite
Strategic risk	Risk relating to prospective earnings and capital arising from strategic changes in the business environment and from adverse strategic business decisions.	Moderate
Operational risk	Risk relating to current operational and financial performance and capital arising from inadequate or failed internal processes, people and systems or external events.	Low - Moderate
Financial risk	Risk relating to financial loss due to the financial structure, cash flows and financial instruments of the business (including capital structure, insurance and fiscal structure) which may impair its ability to provide an adequate return.	Low
Compliance risk	Risk of non-compliance with relevant laws and regulations (including health and safety), internal policies and procedures.	Zero - Low - tolerance

3.1.5. De risicorespons per voornaamste risico maakt duidelijk wat het antwoord op dat risico is

De risicorespons van de onderneming verschaft per specifiek risico belangrijke informatie. Hiermee wordt aangegeven op welke wijze de onderneming het risico mitigeert. Er zijn verschillende typen respons te onderscheiden: ontwijken, overdragen / delen, mitigeren of accepteren. Een risico kan ontweken worden door ervoor te kiezen om bijvoorbeeld niet in een bepaald werelddeel of land de operationele activiteiten uit te breiden. Een onderneming kan er ook voor kiezen een risico te willen nemen maar de gevolgen niet of gedeeltelijk te willen dragen. Door middel van verzekeringen is een

risico tegen kosten over te dragen en door middel van joint ventures, partnerships en contractuele bedingen zijn risico's te delen met een andere partij. Indien een onderneming een risico wil nemen maar de impact of kans van optreden van dat risico wil terugbrengen zijn mitigerende maatregelen mogelijk. Dat neemt niet weg dat het ook mogelijk is dat een onderneming een specifiek risico kan accepteren zonder daar enige actie op te zetten. Die situatie kan zich voordoen wanneer de impact van een risico op de onderneming niet opweegt tegen de kosten om dat risico te verzekeren.

Uit het onderzoek blijkt dat 90% van de ondernemingen in de beschrijving van de risico's per risico een respons publiceert (zie tabel 1). De beschreven respons bestaat uit mitigerende beheersingsmaatregelen voor de meeste of alle risico's. In meer uitzonderlijke gevallen wordt voor een of enkele risico's als respons – in plaats van een mitigerende maatregel – een beschrijving gegeven van het ontwijken van het risico (9%), het overdragen of delen van het risico (27%) of het accepteren van het risico (11%). Ondanks dat 90% van de ondernemingen per risico een risicorespons opnemen, zou men hier een 100% score mogen verwachten. Immers, de respons plaatst het risico dat de onderneming loopt in het juiste perspectief. De verklaring is er deels in gelegen dat de overige 10% tevens ondernemingen bevat die een beursnotering in de US hebben; in de Amerikaanse claimcultuur is het niet gebruikelijk om per risico tevens de risicorespons te benoemen.

Voornamelijk bij ondernemingen die projectmatig werken is een vorm van ontwijken van risico's in de risicoparagraaf beschreven. Zo geeft Arcadis N.V. in haar jaarverslag aan dat een duidelijke risicoafweging per potentiële nieuwe klant en per potentieel nieuw project wordt gemaakt, die resulteert in een go of no-go. Bij een no-go worden de risico's verbonden aan een klant of project ontweken. Bij een go worden de risico's verbonden aan een klant of project teruggebracht tot een voor Arcadis N.V. acceptabel niveau door een serie van in de risicoparagraaf beschreven mitigerende maatregelen (Jaarverslag 2013 Arcadis N.V., p. 45). Een aantal ondernemingen geeft aan zich te verzekeren tegen risico's of op andere wijze risico's

Tabel 1 Risicorespons

	# AEX	# Midcap	# Totaal	% Totaal
Risicorespons per risico opgenomen in risicoparagraaf	21	24	45	90%
Aard van de opgenomen risico respons *)				
- Mitigerende maatregelen	21	24	45	100%
- Ontwijken	0	4	4	9%
- Overdragen/delen	5	7	12	27%
- Accepteren	3	2	5	11%
* voor zover de ondernemingen een risicorespons heeft opgenomen in de risicoparagraaf				

Figuur 5 Voorbeeld mitigerende maatregelen uit jaarverslag 2013 van SBM Offshore N.V., pp. 73, 74

Risk Categories / Risk Factors

Fleet Operations

Example

The operation of offshore production units, presents environmental, performance, health, security and safety risks which must be identified, assessed, and managed.

- Production Operations / Maintenance
- HSSE
- Regulatory Compliance / Local content
- Crisis Management

Response Plan

- Safeguard system uptime by a design process based on direct operating experience. Reliability, Availability and Maintainability (RAM) modelling, planned and preventative maintenance as well as condition-based monitoring are also designed to maximise uptime.
- SBM Offshore has operated FSOs/FPSOs for over 200 contract years, with a total operating downtime of less than 1%.
- Strict operating and Risk Management procedures along with preventive maintenance programs.
- Careful selection and intensive training of high quality personnel.
- A survey program of Hull and Topsides set by the Classification Societies.
- Management system accreditation and compliance with the requirements of the International Safety Management (ISM) Code 2002.
- Proactive regulatory compliance / Training and awareness Crisis
- Management exercise/ training;

over te dragen of te delen. Zo geeft Wolters Kluwer in haar risicoparagraaf bij het operationele risico van technologische ontwikkelingen het volgende aan: “To manage execution risks by third parties, risk transfer and performance management are governed by detailed operating and service agreements with outside providers” (Jaarverslag Wolters-Kluwer N.V. 2013, p. 226). Een voorbeeld van een beschrijving van diverse mitigerende maatregelen als risicorespons per risico wordt gegeven in het jaarverslag van SBM Offshore N.V. (zie figuur 5).

3.1.6 Wordt de risicotrend de nieuwe trend?

Wordt in de risicoparagraaf aandacht besteed aan de beweging in de tijd van het risicoprofiel van de onderneming? Waar de omgeving van de onderneming niet stilstaat en een onderneming haar strategie bijstelt,

is de verwachting dat ook het risicoprofiel door de jaren heen beweegt. Waar in onderzoeken naar risicoparagrafen in de voorbije jaren met regelmaat aandacht wordt geschonken aan de impact en kans van optreden van de risico's, kijkt dit onderzoek in het verlengde daarvan of ook de trend in de tijd – toename of afname van het risico ten opzichte van vorig jaar – wordt aangegeven. Een dergelijke benadering van de risicorapportage past tevens binnen het concept van integrated reporting omdat het de samenhang laat zien tussen ontwikkelingen in de omgeving en/of strategische keuze van de onderneming, haar waardecreërende activiteiten en wat dat betekent voor de risico's die de onderneming loopt (IIRC, 2013). Om die reden kan het inzichtelijk maken van de risicotrend aan te merken zijn als een opkomend ver-

Figuur 6 Voorbeeld risicotrend uit jaarverslag 2013 van Randstad Holding N.V., p. 88

strategic 2013	operational 2013	financial & reporting 2013	compliance 2013
- Adapting to economic conditions - Protecting our reputation	- Contractual liability - Business continuity - Retention of talent	- Credit risk - Other financial reporting risks	- Increased complexity of laws and regulations - Tax compliance - Competition law compliance - Candidate screening - Client claims on French subsidies
strategic 2012	operational 2012	financial & reporting 2012	compliance 2012
- Adapting to economic conditions - Stability of the eurozone - Protecting our reputation ¹	- Contractual liability - Business continuity - Attraction and retention of talent	- Access to funding - Credit risk	- Tax compliance - Competition law compliance - Candidate screening

¹ The risks shown in bold are considered to represent our top risks in 2013 respectively 2012. This list should not be taken as exhaustive.

schijnsel waarmee ondernemingen een volgende stap kunnen maken in de volwassenheid van de risicorapportage aan stakeholders.

Een aantal ondernemingen gaat voortvarend te werk met het inzichtelijk maken van de risicotrend. De risicotrend wordt in meerdere of mindere mate aangeduid in 32% van de onderzochte risicoparagrafen. In de risicoparagraaf van Randstad Holding N.V. geeft deze onderneming per risicocategorie de voornaamste risico's van dit jaar en van vorig jaar. Hiermee geeft zij eenvoudig inzicht in de wijzigingen van het risicoprofiel van de onderneming ten opzichte van het voorafgaande jaar (zie figuur 6). De top vijf à zes risico's zijn voor beide jaren dik gedrukt, wat ook bij herhaling van risico's van het voorafgaande jaar verduidelijkt of dat specifieke risico in belangrijkheid is gedaald, gestegen of gelijk gebleven.

Een ander helder voorbeeld van hoe de trend van het risico gerapporteerd kan worden, wordt gegeven door Ziggo N.V. In haar risicoparagraaf beschrijft zij het risico en de risicorespons. Daarnaast wordt middels een figuur aan de linkerkant aangegeven of het een low, medium of high risk is én wat de risicotrend – stable, increasing, rising – is (zie figuur 7).

3.1.7 Black-box risico's die het bestaansrecht van de onderneming kunnen raken worden zelden genoemd

In haar jaarverslag geeft het bestuur een beschrijving van de voornaamste risico's gerelateerd aan de strategie van de onderneming. Er is een aantal typen risico's dat niet alleen gerelateerd is aan de strategie van de onderneming, maar zelfs in potentie het bestaansrecht van de onderneming, de 'licence to operate' van de onderneming, en de continuïteit in gevaar kan brengen. Dit zijn bij uitstek risico's die de reputatie van de onderneming in de kern kunnen raken, zoals Health, Safety & Environment (HSE) – en compliance-gerelateerde risico's die

naast directe financiële gevolgen zoals een boete, met name hoge indirecte – moeilijk te berekenen – schade geven. Er zijn ruimschoots voorbeelden van ondernemingen die door veiligheidsincidenten, fraudezaken of corruptieschandalen ten onder zijn gegaan of ternauwernood de 'licence to operate' hebben kunnen behouden. De grootste schade wordt bij dergelijke incidenten gevormd door het gebrek aan vertrouwen in de onderneming bij financiers, aandeelhouders, leveranciers, klanten, werknemers en overige stakeholders. De directe financiële schade van een eventuele boete is beperkt in vergelijking tot de grote investering die doorgaans gedaan moet worden in bijvoorbeeld de compliance-infrastructuur om het vertrouwen in de onderneming te herstellen.

In het onderzoek is dan ook de vraag meegenomen of ondernemingen in hun risicoparagraaf aandacht schenken aan risico's die met name de reputatie van de onderneming kunnen schaden. Uit het onderzoek blijkt dat 72% van de onderzochte ondernemingen duidt op de reputatieschade die bepaalde risico's met zich mee kunnen brengen. Zeldzaam is de vermelding dat een risico een dermate hoge impact op de onderneming kan hebben dat het de continuïteit van de onderneming kan raken. Een voorbeeld wordt gegeven in de risicoparagraaf van AkzoNobel N.V. waarin zij bij het productieprocesrisico aangeeft dat grootschalige incidenten op het gebied van persoonlijke gezondheid en veiligheid, procesmatige veiligheid en productveiligheid kunnen resulteren in een risico voor de continuïteit van de onderneming en reputatieschade (Jaarverslag AkzoNobel N.V. 2013, p. 25).

Door de gehele – de financiële en reputatie- – impact van HSE en compliance-gerelateerde risico's te benoemen in de risicoparagraaf, wordt zichtbaar dat deze risico's niet alleen een hygiëne-aspect, een randvoorwaarde, maar ook een strategisch aspect in zich hebben. Het beïnvloedt immers hoe de onderneming gezien wordt

Figuur 7 Voorbeeld risicotrend uit jaarverslag 2013 van Ziggo N.V., p. 49

Operational Risks	Definition	Mitigation
Service Excellence Level - Medium  Trend - Stable 	Our products are at the heart of society and tightly integrated in our customers' day-to-day lives, making service levels, customer satisfaction and service excellence our key priorities. The continuity and quality of our (network) services is the primary condition for providing our services and subject to the highest service levels. Our challenge is to be pro-active and demonstrate customer insight, resulting in an increase in customer satisfaction and with the possibility to clearly distinguish ourselves from our competitors. If, however, our service levels are not met, our customers may not be satisfied by our products or services. This may lead to customer churn or additional costs to maintain our customer base.	We continuously monitor our customer satisfaction using Net Promoter Scores (NPS) as a key indicator. Based on NPS results, we set our priorities for improving our current processes and training our staff. In addition, the implementation of our IT strategy will allow us to be more pro-active and demonstrate customer insight.
	The success of our products depends on, among other things, the quality and variety of the television programming delivered to our subscribers. We do not produce our own content and depend upon broadcasters for programming.	We continuously monitor the quality and variety of the television programming delivered by broadcasters as perceived by our customers. As a result, we have updated our television programming multiple times during 2013.

door haar stakeholders en wat haar rol is in de maatschappij. Het bestaansrecht van de onderneming heeft in feite een stakeholderoriëntatie in plaats van een shareholderoriëntatie en dat is terug te zien in de impact van dit type risico's.

3.2 Beschrijving risicomanagementsysteem

3.2.1 Het blijft zoeken naar wijzigingen en geplande verbeteringen in interne risicobeheersings- en controlesystemen

De Nederlandse Corporate Governance Code vraagt in best practice-bepaling II.1.4 b) in het jaarverslag een beschrijving te geven van de opzet en werking van de interne risicobeheersings- en controlesystemen met betrekking tot de voornaamste risico's van de onderneming in dat specifieke boekjaar. Daarnaast vraagt de code in best practice-bepaling II.1.4 c) een beschrijving te geven van significante wijzigingen die in de systemen zijn aangebracht of belangrijke verbeteringen die zijn gepland. Uit het onderzoek blijkt dat alle ondernemingen die onder de Code vallen een dergelijke beschrijving van de opzet en werking van systemen opnemen.

Het blijft echter zoeken naar aangebrachte significante wijzigingen en/of geplande verbeteringen in de systemen (20%). Dat lijkt de indruk te wekken van vrij stabiele interne risicobeheersings- en controlesystemen. Waar de omgeving, strategie, risicoprofiel en risicotrend van de onderneming elk boekjaar wat kan fluctueren, is het denkbaar dat ook in de opzet en werking van de systemen een wijziging of verbetering dient te

worden aangebracht. Een voorbeeld daarvan wordt gegeven in het jaarverslag van Heijmans N.V. (zie figuur 8) waarin een beschrijving van de aangebrachte wijzigingen in 2013 en geplande verbeteringen voor 2014 van het risicomanagementraamwerk wordt gegeven.

3.2.2 Tekortkomingen worden niet onder de mat geschoven maar je moet wel een goede lezer zijn

De Nederlandse Corporate Governance Code vraagt in best practice-bepaling II.1.4 c) een beschrijving te geven van eventuele belangrijke tekortkomingen in de systemen die in dat boekjaar zijn geconstateerd. Uit het onderzoek blijkt dat tekortkomingen incidenteel (in 18%) worden benoemd in de risicoparagraaf. Belangrijke tekortkomingen worden benoemd door ondernemingen die door incidenten en reputatieschade wat uit te leggen hebben aan de stakeholders. In dergelijke gevallen zijn de tekortkomingen eerder al gecommuniceerd met de stakeholders en worden de tekortkomingen ter volledigheid in het jaarverslag bevestigd, inclusief de wijze waarop wordt omgegaan met die tekortkomingen. Voorbeelden hiervan zijn te vinden in het jaarverslag van Koninklijke Imtech N.V. en Brunel (Jaarverslag 2013, p. 69). In zeven andere jaarverslagen worden ook minder belangrijke tekortkomingen benoemd. Bijvoorbeeld DSM rapporteert onder de noemer van 'what still went wrong in 2013' een aantal kleinere incidenten en Randstad rapporteert over een aantal – niet materiële – gedetecteerde fraudes (Jaarverslag 2013, p. 87).

Figuur 8 Voorbeeldfragmenten van aangebrachte wijzigingen in én geplande verbeteringen van de systemen uit jaarverslag 2013 van Heijmans N.V., pp. 72-75

Risk management in 2013 A number of items of attention in relation to risk management for the coming years were formulated in the 2012 annual report. The following measures and actions were taken in this context in 2013:	Focus of risk management in 2014 Many of the items of attention and actions in 2013 will be followed up in 2014, with the addition of certain other actions and/or measures. In practice, this means: • Risk management with respect to complex projects in all segments will be further intensified, with adequate attention from the Executive Committee and corporate control; • Continuation of the 'fit for Cash' programme and the realisation of the divestment programme at Property Development; • Continuation of the implementation of the 'improve the core' programme with respect to tender management, project management, procurement and sales; • Continuation of the GO! safety programme; • Improvement of the reporting structure with respect to cross-sector projects or projects involving parties outside the Group; • Review of the risk framework with input from the 'improve the core' programme;
• The company-wide risk management audits continued in 2013, with specific attention to the management of project risks during the acquisition and preparatory phase. In addition, these audits now include attention to compliance with the law on foreign workers and the risks relating to chain and hiring liability as a permanent item.	
In general, with respect to 2013 one can conclude that the proposed measures were actually implemented. We are convinced that over time, this will also contribute to the company's result. The focus of risk management remains on the management of projects. Several larger	

3.3 De In-control-verklaring

Het onderzoek toont het volgende beeld, uitgewerkt in paragraaf 3.3.1 t/m 3.3.3.

3.3.1 Bewust of onbewust worden In-control-verklaringen afgegeven met een bredere scope dan de Code verlangt

Best practice-bepaling II.1.5 in de Code vraagt van Nederlandse beursgenoteerde NV's dat het bestuur een In-control-verklaring afgeeft: "ten aanzien van financiële verslaggevingsrisico's verklaart het bestuur in het jaarverslag dat de interne risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat en dat de risicobeheersings- en controlesystemen in het verslagjaar naar behoren hebben gewerkt. Het bestuur geeft hiervan een duidelijke onderbouwing." Opgemerkt wordt dat buitenlandse entiteiten niet onder de Nederlandse Code vallen, maar ingevolge een US-beursnotering gehouden kunnen zijn aan de Sarbanes Oxley-404 In-control-verklaring. Deze SOx 404-verklaring is een In-control verklaring over de effectieve opzet, bestaan en werking van het systeem van interne beheersing rondom de financiële verslaggeving per ultimo boekjaar.

De In-control-verklaring beperkt zich volgens de Code tot de interne beheersing van de financiële verslaggevingsrisico's. Opvallend is het daarom dat drie van de AEX- en twaalf van de AMX-fondsen een in-control-verklaring afgeven die ook op een aantal of alle andere risicogebieden, zoals strategisch, financieel, operationeel en compliance, betrekking heeft. Binck Bank N.V. is een voorbeeld van een onderneming die in haar jaarverslag 2013 een specifieke, duidelijk gedefinieerde, maar bredere In-control verklaring heeft opgenomen; dit in lijn met de COSO-ERM (COSO, 2004) benadering.

Een aantal andere ondernemingen daarentegen expliciteert de scope niet, en roept daarmee het beeld op dat de In-control-verklaring betrekking heeft op alle risicogebieden. Dat kan bewust zijn maar dat kan ook onbewust zijn doordat de zinsnede 'ten aanzien van de financiële verslaggevingsrisico's' niet is opgenomen. Bewust of onbewust gaan dus een behoorlijk aantal Nederlandse ondernemingen qua scope met hun In-control-verklaring verder dan de Code vereist sinds 2009. Dat is opvallend want hiermee lopen organisa-

ties een groter (bestuurders-)aansprakelijkheidsrisico en gaat een aantal ondernemingen voorbij aan de argumentatie die juist ten grondslag lag aan de keuzes van de Commissie Frijns om de scope van de In-control-verklaring van een brede scope (alle risicocategorieën) terug te brengen naar sec de financiële verslaggevingsrisico's (De Groot & Koolstra, 2006).

Opvallend is tevens dat nog steeds een aantal ondernemingen tevens een forward looking statement opneemt in de In-control-verklaring. De forward looking statement – geïntroduceerd door de Monitoring Commissie Corporate Governance Code in haar jaarrapport van 2005 – houdt in dat expliciet gesteld wordt dat er wordt verklaard dat er geen indicaties zijn dat de risicobeheersings- en controlesystemen in het lopende jaar niet naar behoren zullen werken. Sinds de aanpassing van de Code door de commissie Frijns is de forward looking statement vanaf 2009 niet langer in de relevante best practice-bepaling opgenomen.

Tenslotte, de In-control-verklaring in het jaarverslag 2013 van Randstad en KPN kunnen als good practices worden aangemerkt. Zo stelt KPN het volgende: "With reference to best practice provision II.1.5 of the Dutch Corporate Governance Code, the Board of Management, to the best of its knowledge, believes that the Internal Risk Management and Control System, with regard to financial reporting, worked properly in 2013 and that the Internal Risk Management and Control System provides a reasonable assurance that the financial reporting does not contain any errors of material importance" (KPN, Jaarverslag 2013, p. 69).

3.3.2 Scope In-control-verklaring: effectieve werking interne beheersing

De meeste In-control-verklaringen uitgebracht door de onderzochte ondernemingen die vallen onder de Nederlandse Code, bevatten een expliciete verklaring dat de interne beheersing naar behoren heeft gewerkt. Slechts één van deze onderzochte directieverslagen hanteert deze bewoordingen niet expliciet.

Met uitzondering één onderneming maakt geen enkele Nederlandse NV die in verband met een beursnotering in de US tevens moet voldoen aan de Sarbanes Oxley 404-regelgeving, gebruik van de mogelijkheid die de Code sinds de aanpassingen van Frijns biedt om de

Figuur 9 Voorbeeld bredere In-control-verklaring uit het jaarverslag 2013 van Binck Bank N.V., p. 106

In accordance with the best practice provisions as stated in the Corporate Governance Code and with due observance of the limitations stated below, we confirm that our risk management and control systems provide a reasonable level of security and that we are aware:

- of the extent to which BinckBank's strategic and operational targets are achieved;
- that BinckBank is in compliance with the applicable legislation and regulation; and
- that our financial reporting is free from material misstatements.

We moreover declare that these risk management and control systems have performed satisfactorily in 2013.

SOx 404 In-control-verklaring ten aanzien van de beheersing van de financiële verslagleggingsrisico's ook te gebruiken voor het voldoen aan de Nederlandse In-control-verklaring conform best practice-bepaling II.1.5.; dit overigens ondanks het verschil dat de SOx 404-verklaring betrekking heeft op de situatie ultimo boekjaar en de Nederlandse verklaring betrekking heeft op het gehele verslagjaar (De Groot & Koolstra, 2007). In het jaarverslag van Unilever en Philips zijn zowel de SOx 404-verklaring als de Nederlandse In-control-verklaring opgenomen, waarbij bij de Nederlandse verklaring overigens wel een disclaimer is toegevoegd dat die Nederlandse verklaring niet opgevat moet worden als een SOx 404-verklaring.

3.3.3 Clausulering van de In-control verklaring is hoge uitzondering

Eén onderneming die een In-control-verklaring afgeeft clauseert deze verklaring, met andere woorden, geeft een niet schone In-control-verklaring af. Met een niet schone In-control-verklaring wordt in dit kader bedoeld een In-control-verklaring waarin de conclusie wordt geclausuleerd door te stellen dat het systeem heeft gewerkt met uitzondering van de materiële tekortkoming in het systeem; of dat wordt gesteld dat het gehele systeem niet naar behoren heeft gefunctioneerd omdat er sprake was van een of meerdere materiële tekortkomingen. Zo stelt deze onderneming het volgende: "In view of the events that have come to light it is clear that our risk management and internal control systems had not functioned at an adequate level. Shortcomings in project control, oversight and culture have been determined."

4 Aanbevelingen

4.1 Aanbevelingen aan de opstellers

Er zijn - mede gezien de geschetste ontwikkelingen in regelgeving en stakeholderverwachtingen en de resultaten van het onderzoek naar de risicoparagrafen van de 50 AEX- en AMX-ondernemingen - een aantal onderwerpen die om nadere aandacht vragen van de opstellers van de risicoparagraaf. De voornaamste aanbevelingen zijn:

- breng een expliciete koppeling aan tussen strategische doelstellingen, waardecreatie en individuele risico's (zie paragraaf 3.1.1);
- benoem de risicohouding (zie paragraaf 3.1.4);
- duidt aan wat de toprisico's zijn (zie paragraaf 3.1.2);
- benoem de trend in het risico in de tijd (zie paragraaf 3.1.6);
- benoem belangrijke doorgevoerde c.q. geplande verbeteringen in het systeem van risicomanagement (zie paragraaf 3.2.1);
- kijk kritisch naar de reikwijdte van de In-control-verklaring en formuleer de In-control-verklaring scherp (zie paragraaf 3.3.1);
- vorm en stijl doen er echt toe: veel grote (doorgaans

AEX-genoteerde) ondernemingen hebben een mooie visuele risicoparagraaf die de leesbaarheid ten goede komt;

- bewaak de samenhang tussen de risicoparagraaf, het verslag van de Raad van Commissarissen (RvC) en de nieuwe controleverklaring van de externe accountant (zie paragraaf 1).

4.2 Aanbevelingen aan de interne toezichthouders

Naast de bovengenoemde aanbevelingen voor de opstellers van de risicoparagraaf, zijn er uit de resultaten van het onderzoek, en gezien hun toezichtsrol op risico's en risicomanagement inclusief de verantwoording daarover door de raad van bestuur, ook een aantal specifieke aandachtspunten te benoemen voor de interne toezichthouders (commissarissen) op de risicoparagraaf in het jaarverslag. Deze voornaamste aanbevelingen zijn:

- stel kritische vragen over de breedte, scherpheid en trend in de tijd van het risicoprofiel;
- stel vast dat de externe verslaglegging aansluit op de interne verslaglegging over risico's en risicomanagement;
- ga de discussie aan over wat (materiële c.q. belangrijke) geconstateerde tekortkomingen en geplande verbeteringen zijn en over redenen om die wel/niet te benoemen in de risicoparagraaf;
- benoem in het verslag van de RvC / Audit committee de voornaamste risico's samenhangend met de financiële verslaglegging en tevens dat deze zijn besproken met de externe accountant.

4.3 Ten slotte

Bij het opstellen van de risicoparagraaf moet niet voorbij worden gegaan aan het risico van de risicoparagraaf zelf: namelijk de zaken mooier voorstellen dan ze zijn. Ook dient geborgd te zijn dat de externe risicoparagraaf voortbouwt op reeds beschikbare interne informatie die tevens is besproken met de Raad van Commissarissen. Wij verwachten dat naar de toekomst toe – bijvoorbeeld in lijn met de ontwikkeling rondom de governance code in de UK – commissarissen meer dan nu aangesproken zullen gaan worden op hun toezichthoudende taak ten aanzien van risico's, risicohouding en risicomanagement.

De externe verslaglegging kan de aanjager zijn voor het intern vergroten van de inspanning op het terrein van risicomanagement en risicoverslaglegging. De risicoparagraaf in het directieverslag zal ook volgende jaren in beweging blijven. Met dit artikel streven de auteurs een beeld te geven van de potentie tot verbetering die de risicoparagraaf van het jaarverslag geeft. Oftewel, wat de volgende stap is die een aantal ondernemingen kunnen maken in het tegemoetkomen aan de actuele wensen van stakeholders. Het mooiste resultaat dat dit artikel kan opleveren is dat u leert van anderen of zelf de ambitie benoemt om een voorbeeld te worden voor anderen.

Mr. dr. M.M.A. (Marijn) van Daelen is verbonden aan Tilburg University en werkzaam bij Deloitte Risk Services B.V. en zij heeft zich gespecialiseerd in ondernemingsrecht, corporate governance, risicomanagement en compliance.

Drs. J.I. (Jos) de Groot RA is werkzaam als senior director in de Assurance praktijk van PwC en is als accountant/adviseur

actief op het terrein van corporate governance, risk en compliance.

Wij danken Jeroen Bellinga, Patrick Schouwenburg, Nessar Soltan-Ali en Joes van Berkel voor hun bijdrage als onderzoeksassistenten aan dit onderzoek.

Literatuur

- Brouwer, A.J., & Groot, J.I. de (2014). Nieuwe controleverklaring daagt commissaris uit. *Het Financieele Dagblad*, 24 april 2014.
- COSO (2004). Enterprise Risk Management – Integrated Framework: Executive summary, 3. Geraadpleegd op www.coso.org.
- Daelen, M. van (2013). Een format voor de openbaarmaking van risico-informatie. *Maandblad voor Accountancy en Bedrijfseconomie*, 87(7/8), 316-324.
- Daelen, M. van (2012). Risk management and corporate governance: Match between the legal framework and practice. Brugge: Die Keure.
- Deloitte (2009). Risicomanagement: meer dan de som der delen. Geraadpleegd op www.deloitte.nl.
- Deloitte (2013). Risicoparagraaf mist aansluiting met strategie: Ontwikkeling risicoparagrafen 2012. Geraadpleegd op <http://actueel.deloitte.nl/newsroom/persberichten/risicoparag>
- portage-in-jaarverslag-mist-aansluiting-met-strategie.
- De Nederlandsche Bank (2011), Open Boek Toezicht, vraag & antwoord. Geraadpleegd op www.toezicht.dnb.nl.
- Eumedion (2013). Eumedion Focus Letter 2014. Geraadpleegd op www.eumedion.nl.
- Eumedion (2014). Eumedion Focus Letter 2015. Geraadpleegd op www.eumedion.nl.
- Groot, J.I. de (2010). Op weg naar een raamwerk voor risicoverslaglegging. *Tijdschrift voor jaarrekeningrecht*, Nr. 1-2, april 2010, jaargang 5, 38-47.
- Groot, J.I. de, & Koolstra, B. (2007). Eén 'in control'-statement vaak afdoende. *CFO Magazine*, juli-augustus.
- Groot, J. de, en Koolstra, B. (2006). De 'in control' good practice van de Commissie Frijns lost slechts een deel van de puzzel op. *Maandblad voor Accountancy en Bedrijfseconomie*, 80(7/8), 392-400.
- International Integrated Reporting Council (IIRC) (2013). The International Integrated Reporting <IR> framework. Geraadpleegd op www.theiirc.org
- NBA (2014). Transparant over de controle: Consultatiedocument uitgebreidere controleverklaring. Geraadpleegd op www.nba.nl.
- Nederlandse Corporate Governance Code: Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen. Geraadpleegd op www.commissiecorporategovernance.nl.
- PwC (2014). Klare Taal! Benchmark controleverklaring 'nieuwe stijl' onder Nederlandse beursfondsen. Geraadpleegd op www.pwc.nl/nl_NL/nl/assets/documents/pwc-klare-taal.pdf.
- Vereniging van Effectenbezitters (2013). VEB speerpuntenbrief 2014. Geraadpleegd op www.veb.nl.

Bijlage A Lijst van onderzochte ondernemingen (AEX en Midkap fondsen naar de stand per 1 januari 2014)

AEX fondsen:	Midcap fondsen:
AEGON N.V.	Aalberts Industries N.V.
Air-France-KLM	AMG Advanced Metallurgical Group N.V.
Akzo Nobel N.V.	Aperam
ArcelorMittal	ARCADIS N.V.
ASML Holding N.V.	ASM International N.V.
Corio N.V.	BinckBank N.V.
Fugro N.V.	Brunel International N.V.
Gemalto N.V.	Corbion N.V.
Heineken N.V.	Delta Lloyd N.V.
Imtech N.V.	Eurocommercial Properties N.V.
ING Groep N.V.	Heijmans N.V.
Koninklijke Ahold N.V.	Koninklijke BAM Groep N.V.
Koninklijke DSM N.V.	Koninklijke Boskalis Westminster N.V.
Koninklijke KPN N.V.	Koninklijke Ten Cate N.V.
Koninklijke Philips Electronics N.V.	Koninklijke Vopak N.V.
PostNL N.V.	Nieuwe Steen Investments N.V.
Randstad Holding N.V.	Nutreco Holding N.V.
Reed Elsevier N.V.	OCI Nitrogen
Royal Dutch Shell A	Pharming Group N.V.
SBM Offshore N.V.	TKH Group N.V.
TNT Express N.V.	Tomtom N.V.
Unibail-Rodamco	UNIT4 N.V.
Unilever N.V.	USG People N.V.
Wolters Kluwer N.V.	VastNed Retail N.V.
Ziggo N.V.	Wereldhave N.V.